REMARKS

Claims 1, 2, 4-10, 12-31, 33-37 and 39 remain pending in the application. Reconsideration is respectfully requested in light of the following remarks.

Objection to the Specification

In regard to the Examiner's objection to the specification, the functionality described by the means limitations of claim 15 is clearly described in Applicant's specification in regard to payment device 100 (*see e.g.,* Figure 1 (item 100), Figure 3, Figure 4, and associated descriptions). Thus, it is clearly the payment device that corresponds to the various means. Furthermore, the functionality described by the means limitations of claim 39 is clearly described in Applicants specification in regard to credit company computer 330 of Figure 5 (*see e.g.,* Figure 3, item 332; Figure 5, item 330; and associated descriptions). Accordingly, Applicants respectfully request removal of the Examiner's objection.

Section 112, Second Paragraph, Rejection:

The Examiner rejected claims 15 and 39 under 35 U.S.C. § 112, second paragraph as indefinite. Applicant's traverse the rejection for at least the reasons presented below.

In regard to claim 15, Applicants assert that it is clear from Applicant's specification that the corresponding structure for the means limitations of claim 15 is payment device 100 (*see e.g.,* Figure 1 (item 100), Figure 3, Figure 4, and associated descriptions). Furthermore, in regard to claim 39, Applicants assert that it is clear from Applicant's specification that the corresponding structure for the means limitations of claim 39 is database 332 of Figure 3 and computer 330 of Figure 5 (*see e.g.,* Figure 3, item 332; Figure 5, item 330; and associated descriptions). Accordingly, Applicants respectfully request removal of the Examiner's rejection.

Section 103(a) Rejection:

The Examiner rejected claim 1, 2, 4-8, 9-14, 16, 26, 28 and 29 under 35 U.S.C. § 103(a) as being unpatentable over Walker et al. (U.S. Publication 2006/02180980 (hereinafter "Walker") in view of Wynn (U.S. Patent RE38,137 E), claims 15, 17-25, 30, 31, 33-37 and 39 as being unpatentable over Walker in view of Sarcanin (U.S. Publication 2005/0246292), claim 6 as being unpatentable over walker in view of Mann, III, et al. (U.S. Publication 2006/0122943) (hereinafter "Mann"), claim 8 as being unpatentable over Walker in view of Pitroda (U.S. Publication 2005/0247777), claim 24 as being unpatentable over Walker in view of Sarcanin and further in view of Wynn, and claim 27 as being unpatentable over Walker in view of Wynn and further in view of Sarcanin.

Claim 1

In regard to claim 1, Walker and Wynn, taken singly or in combination, fail to teach or suggest a communications facility operable to communicate with a terminal, wherein the apparatus is operable to a) receive bill details for a transaction from the terminal through the communications facility b) generate a transaction record from the bill details [received from the terminal], and c) transmit the transaction record to the same terminal through the communications facility. Thus, according to the specific limitations of claim 1, the apparatus is operable to receive bill details for a transaction from the terminal through the communications facility, generate a transaction record from the bill details [received from the same terminal], and transmit the transaction record to the same terminal through the communications facility. Neither Walker nor Wynn, taken singly or in combination, teach or suggest such an apparatus. The Examiner acknowledges that Walker fails to disclose an apparatus operable to receive bill receive bill details for a transaction from the terminal through the communications facility; the Examiner relies on Wynn to disclose this limitation. The Examiner cites Figure 6 and column 2 (lines 25-35 and 40-50) of Wynn. Figure 6 of

Wynn illustrates examples of fields that make up a financial transaction record in Wynn's system. Column 2 of Wynn does disclose that his universal financial data card (UFDC) includes a processor capable of "compil[ing] a transaction record." However, nowhere does Wynn (even when combined with the teachings of Walker) teach or suggest transmitting his transaction record to the same terminal from which bill details for the transaction are received. Column 2, lines 30-32 of Wynn disclose that his transaction records may be "compiled from financial transaction data communicated between the universal financial data card and a card reader" (emphasis added). Presumably, the Examiner considers such card reader to be equivalent Applicant's claimed terminal. **However, nowhere does Wynn (even when combined with the teachings of Walker) teach or suggest transmitting his transaction record to the same card reader from which his "financial transaction data" is received.** Accordingly, Wynn and Walker, taken singly or in combination, fail to teach or suggest receiving bill details for a transaction from the terminal through the communications facility, generating a transaction record from the bill details, and transmitting the transaction record to the *same* terminal through the communications facility.

Moreover, Applicants note that Wynn describes various versions of his card reader. For instance, in Figure 3 and associated description, Wynn describes a "financial institution version of the card reader." In Figure 4 and associated description, Wynn describes a "merchant/commercial institution version of the card reader." Additionally, in Figure 5 and associated description, Wynn describes a "residential version of the card reader." **While Wynn describes various versions of his card reader (each having distinct functionality), nowhere does Wynn (even when combined with Walker) disclose that his UFDC interacts with a particular version of his card reader according to the specific limitations of claim 1.** More specifically, nowhere does Wynn (even when combined with the teachings of Walker) teach or suggest that his UFDC receives bill details for a transaction from a particular version of his card reader (which, presumably, the Examiner equates to Applicant's claimed terminal) through the communications facility and transmits the transaction record to the same version of his card reader through the communications facility.

For instance, in regard to the "merchant/commercial institution version" of his card reader, Wynn discloses:

> Advantageously, memory circuit 384 may also be used to store the name of the commercial establishment at which card reader 202 is located, as well as the date, the time, the type of goods or services purchased by the holder of UFDC 201, for transmitting that data to UFDC 201 to be included in the stored financial transaction record. In this manner, this information does not have to be manually keyed in by the operator of card reader 202 for every transaction. Alternatively, that data may be entered manually via keypad 372 which, in one embodiment, represents an alpha-numeric keypad. (column 9, lines 46-56, emphasis added)

As demonstrated above, Wynn discloses that the "merchant/commercial institution version" of his card reader may transmit various information to the UFDC including store name, date, time, as well as the type of goods or services purchased. However, nowhere does Wynn (even when combined with the teachings of Walker) disclose that a transaction record generated from such information is transmitted to the "merchant/commercial institution version" of his card reader.

In further example, in regard to the "residential version" of his card reader, Wynn discloses:

> FIG. 5 shows a residential version of card reader 202 in accordance with one aspect of the present invention. Note that card reader 202 of FIG. 5 preferably does not include the frequency select circuit 350 (seen in FIGS. 3 and 4), since there is typically only one card reader residing at the card holder's residence. Via computer 370, the card holder can retrieve account information such as balance, payable party, date, amount, checks written, monthly/yearly statements, monthly/yearly spreadsheet, and to perform operations involving the financial accounts stored in UFDC 201, such as home banking, automatic payments, and the like. (column 9, lines 57-67, emphasis added)

As demonstrated above, the card holder can retrieve account information via a computer coupled to the "residential version" of the card reader; however, nowhere does Wynn (even when combined with the teachings of Walker) teach or suggest that account information is received from the "residential version" of the card reader. Applicant's also

note that the description of "account information" above does not include Wynn's "transaction records."

Since Wynn (even when combined with the teachings of Walker) fails to teach or suggest that his UFDC receives bill details for a transaction from a particular version of his card reader and transmits the transaction record to the same version of his card reader, Wynn and Walker cannot be said to teach the specific limitations of claim 1 including a communications facility operable to communicate with a terminal, wherein the apparatus is operable to a) receive bill details for a transaction from the terminal through the communications facility b) generate a transaction record from the bill details [received from the terminal], and c) transmit the transaction record to the same terminal through the communications facility.

Furthermore, Walker's device is not operable to communicate with a terminal. The Examiner cites paragraph [0004] which mentions "wireless connection." However, such "wireless connection" pertains to the communication between a merchant and a central database. The "wireless connection" has nothing to with functionality of Walker's device. The Examiner further cites the phrase "cardholder transmits the single use number to merchant." Presumably, the Examiner is referring to Figure 3A, which illustrates the cardholder, not Walker's device, transmitting a single-use credit card number to a merchant. In fact, by explicitly teaching that communication with merchants is a responsibility of the cardholder, Walker actually **teaches away** from an apparatus that includes a communications facility operable to communicate with a terminal.

Accordingly, one skilled in the arts of cryptography and security would recognize that it does not makes sense to modify the teachings of Walker with the teachings of Wynn to enable Walker's device to communicate with a terminal, much less utilizing such a communications facility as specified by the limitations of claim 1. More specifically, one skilled in the arts of cryptography and security would recognize that including a communication facility operable to communicate with a terminal would undermine the security of user accounts in Walker's system by potentially exposing the

nonce to third parties through such a communications facility. Walker teaches that his nonce is stored in device memory 104 (, *see e.g.,* paragraph [0053]). Walker also teaches that "[w]hile an attacker cannot generate a valid credit card number without knowledge of the user's private key, knowing the user's nonce undermines the security of the account." Accordingly, adding a communications facility operable to communicate with a terminal would unnecessarily expose Walker's nonce, which is stored in memory 104, to external systems thereby potentially undermining the security of user accounts in Walker's system. Accordingly, one skilled in the art would explicitly avoid modifying the teachings of Walker with the teachings of Wynn, which includes a UFDC configured to communicate with external systems (e.g., Wynn's card reader, computer 370, etc.).

Applicants further assert that the Examiner has not stated a proper reason as to why one of ordinary skill in the art would be motivated to combine the teachings of Wynn with the teachings of Walker. The Examiner asserts:

> Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Walker et al and incorporate the apparatus, wherein the apparatus is operable to: receive bill details for a transaction from the terminal through the communications facility in view of the teachings of Wynn, because such will ensure transaction record tracking. (emphasis added)

However, one seeking to "ensure transaction record tracking" would simply use the teachings of Wynn. The Examiner has merely stated a reason for one skilled in the art to use the teachings of Wynn, not a reason to combine the teachings of Wynn with the teachings of Walker in such a way that would result in Applicant's claimed invention.

Thus, for at least the reasons presented above, the rejection of claim 1 is unsupported by the cited art and removal thereof is respectfully requested. Similar remarks apply to claim 9 and 26.

Claim 15

Walker and Sarcanin (taken singly or in combination) fail to teach or suggest means for creating a respective transaction record for each of the plurality of transactions, wherein the respective transaction comprises a digital signature that is generated using a cryptographic key. The Examiner acknowledges that Walker fails to teach or suggest these limitations; the Examiner relies on Sarcanin to teach the limitations. The Examiner cites [0027], which is reproduced below:

> sending a debit request message from the client terminal to the payment server in response to the draw request message, the debit request message including a first digital signature, the first digital signature for verifying that the debit request message originated from the client terminal, the first digital signature being generated at the client terminal using the smart card information stored at the client terminal; (emphasis added)

While Sarcanin teaches a "debit request message" that includes a digital signature, Sarcanin's "debit request message" is not the same as a *transaction record,* much less a respective transaction record comprising a digital signature that is generated using a cryptographic key. In fact the "debit request message" is generated before any associated transaction has been fully processed as illustrated by paragraph [0029], which describes Sarcanin's authentication server checking the debit request message before the transaction can proceed.

Thus, for at least the reasons presented above, the rejection of claim 15 is unsupported by the cited art and removal thereof is respectfully requested.

Claim 16

In regard to claim 16, Applicant's assert the Examiner has not even attempted to state a *prima facie* rejection of claim 16. The Examiner rejects claim 16 under the same rational as claim 1; however, the limitations of claim 16 substantially differ from the limitations of claim 1. More specifically, claim 16 recites a processor operable to randomly or pseudo-randomly select one identifier from said set of multiple

identifiers for use in any transaction, whereas claim 1 does not. Furthermore, Applicants assert neither Walker nor Wynn (taken singly or in combination) teach or suggest a processor operable to randomly or pseudo-randomly select one identifier from said set of multiple identifiers for use in any transaction.

Thus, for at least the reasons presented above, the rejection of claim 16 is unsupported by the cited art and removal thereof is respectfully requested.

Claim 17

In regard to claim 17, Walker and Sarcanin (taken singly or in combination) fails to teach or suggest receiving a public key from the portable transaction device, receiving a transaction record comprising a digital signature from the portable transaction device, and decrypting and validating the digital signature with the public key. In regard to receiving a public key *from the portable transaction device*, the Examiner cites paragraph [0009] and [0023] of Walker which are reproduced below:

> In addition, credit card information and transaction information may be encrypted using well known encryption schemes like RSA's public key cryptography. For example, SET is a joint Visa/MasterCard standard for encrypting credit card numbers transmitted over the Internet. (paragraph 0009)
>
> According to another aspect of our invention, a device for facilitating credit transactions is provided which includes a processing unit including a cryptographic processor. The device also includes an input unit connected to the processing unit for inputting information thereto, and a display unit connected to the processing unit for displaying a processing result. In addition, the device includes a memory device connected to the processing unit. The memory device contains a private cryptographic key, a first data element, a second data element and a program adapted to be executed by the processing unit. In accordance with the program, the processing unit encrypts the first data element using the private cryptographic key and the second data element, modifies the second data element, combines the encrypted first data element and the second data element to generate a single-use financial account identifier, and displays the single-use financial account identifier using the display unit. (paragraph 0023)

Applicants assert that, while mentioning public key cryptograph, paragraph [0009] fails to mention anything about receiving a public key from a portable transaction device. Furthermore, paragraph [0023] describes Walker's device generating and displaying a single-use financial account identifier. **However, Walker fails to mention anything about his device providing a public key. Additionally, Walker fails to mention anything about his device receiving a public key.** Accordingly, the Examiner's reliance on Walker to teach *receiving a public key from a portable transaction device* is improper.

Walker and Sarcanin (taken singly or in combination) fail to teach or suggest receiving a transaction record comprising a digital signature from the portable transaction device, and decrypting and validating the digital signature with the public key (received from a portable transaction device). The Examiner acknowledges that Walker fails to teach or suggest these limitations; the Examiner relies on Sarcanin to teach the limitations. The Examiner cites [0027], which is reproduced below:

> sending a debit request message from the client terminal to the payment server in response to the draw request message, the debit request message including a first digital signature, the first digital signature for verifying that the debit request message originated from the client terminal, the first digital signature being generated at the client terminal using the smart card information stored at the client terminal; (emphasis added)

While Sarcanin teaches a "debit request message" that includes a digital signature, Sarcanin's "debit request message" is not the same as a *transaction record,* much less a transaction record provided by a portable transaction device. In fact the "debit request message" is generated before any associated transaction has been fully processed as illustrated by paragraph [0029], which describes Sarcanin's authentication server checking the debit request message before the transaction can proceed.

In regard, to *decrypting and validating the digital signature with the public key (received from a portable transaction device),* the Examiner cites paragraph [0095] of Sarcanin. However, paragraph [0095] fails to mention anything about decrypting and

validating the digital signature of Sarcanin's debit request message (on which the Examiner presumably relies to teach Applicants claimed transaction record comprising a digital signature. Instead, at paragraph [0029], Sarcanin discloses:

> comparing at the authentication server the first digital signature contained in the debit request message to a first check digital signature generated at the authentication server using the smart card information stored at the authentication server to determine if the transaction can proceed, the transaction being terminated and a second termination message being sent from the authentication server to the client terminal for display to the user if the first digital signature does not match the first check digital signature;

As demonstrated above, instead of *decrypting and validating* the digital signature *with a public key received from a portable transaction device*, Sarcanin teaches *comparing* the digital request message's digital signature to a digital signature generated at the authentication server *using the smart card information stored at the authentication server*. Clearly, decrypting and validating the digital signature with a public key received from a portable transaction device is not the same as comparing the digital request message's digital signature to a digital signature generated at the authentication server using the smart card information stored at the authentication server.

Furthermore, Applicants further assert that the Examiner has not stated a proper reason as to why one of ordinary skill in the art would be motivated to combine the teachings of Sarcanin with the teachings of Walker. The Examiner asserts:

> Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Walker et al and incorporate the method, wherein receiving a transaction record comprising a digital signature from the portable transaction device, and decrypting and validating the digital signature with the public key in view of the teachings of Sarcanin, because such will ensure adequate transaction security.

However, one seeking transaction security would simply use the teachings of Sarcanin. The Examiner has merely provided a reason as to why one skilled in the art would use the teachings of Sarcanin, not combine the teachings of Sarcanin with the teachings of Walker to produce Applicant's claimed invention. Furthermore, Applicants assert that

the Examiner has not stated a proper reason as to why one of ordinary skill in the art would be motivated to combine the teachings of Sarcanin with the teaching of Walker. The Examiner asserts it would have been obvious to perform such a combination to "...ensure adequate transaction security." However, no one of ordinary skill in the art would modify the teaching of Walker with any other reference to "ensure adequate transaction security" since the primary purpose of Walker's system is to provide adequate transaction security through the use of single use financial account identifiers, which can only be used for one transaction (thereby providing transaction security against stolen or compromised account identifiers). Accordingly, one skilled in the art would not modify the teachings of Walker with any other reference, much less modify the teachings of Walker in such a way that would result in Applicant's claimed invention.

Thus, for at least the reasons presented above, the rejection of claim 17 is unsupported by the cited art and removal thereof is respectfully requested.

Claim 30

In regard to claim 30, the cited art does not teach receiving a request for a transaction on a customer account, wherein the request comprises a digital signature generated by a transaction device associated with the customer account, verifying the digital signature, accessing an identifier within the request, determining which set of multiple identifiers the accessed identifier belongs to, and from this determining a customer account for the transaction, and updating the determined customer account in respect of the transaction. The Examiner attempts to combine the use of a digital signature in Sarcanin with Walker's teachings. However, such a modification to Walker's teachings would not make sense. The primary purpose of Walker's system is to provide adequate transaction security through the use of single use financial account identifiers, which can only be used for one transaction (thereby providing transaction security against stolen or compromised account identifiers). Since the identifiers are single use, there would be no need to apply a digital signature.

Applicants assert that the Examiner has not stated a proper reason as to why one of ordinary skill in the art would be motivated to combine the teachings of Sarcanin with the teaching of Walker. The Examiner asserts it would have been obvious to perform such a combination to "...ensure adequate transaction security." However, no one of ordinary skill in the art would modify the teaching of Walker with any other reference to "ensure adequate transaction security" since the primary purpose of Walker's system is to provide adequate transaction security through the use of single use financial account identifiers, which can only be used for one transaction (thereby providing transaction security against stolen or compromised account identifiers). Accordingly, one skilled in the art would not modify the teachings of Walker with any other reference, much less modify the teachings of Walker with the teachings of Sarcanin in such a way that would result in Applicant's claimed invention.

Thus, for at least the reasons presented above, Applicants assert the Examiner's rejection of claim 30 is improper and removal thereof is respectfully requested. Similar remarks apply to claims 36 and 39.

CONCLUSION

Applicants submit the application is in condition for allowance, and notice to that effect is respectfully requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5681-20500/RCK.

Respectfully submitted,

/Robert C. Kowert/
Robert C. Kowert, Reg. #39,255
Attorney for Applicants

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: November 19, 2007